ABSTRACT

A method for providing secure transactions generates a Secure Card Number ("SCN") for a first entity that is transferred with a first entity identifier to a second entity and then to a money source that verifies that the transaction is valid by use of the first entity identifier and the SCN. The SCN includes a Transaction Information Block ("TIB"), a Counter Block, and an encrypted Personal Identification Number ("PIN") Block. The SCN is transferred to the money source in an account number or a non-account data field. The money source can use the TIB to determine whether the SCN should be used once or multiple times or to identify one of several physical devices, all of which are issued to the first entity, used to generate the SCN. The money source validates the SCN by duplicating the encryption process used to create an encrypted PIN Block and comparing the result to the encrypted PIN Block received with the transaction. A Triple Data Encryption Standard algorithm encrypts a PIN Block generated from a PIN, a Sequence Insertion Number ("SIN") and a known starting value. The SIN can be a combination of three seed values and a random value generated by a Pseudo Random Number Generator ("PRNG") initialized with the seed values. A Counter value is associated with the Counter Block and the seed values.